Topics in Logic and Complexity

Handout 4

Anuj Dawar

http://www.cl.cam.ac.uk/teaching/1920/L15

Expressive Power of Logics

We have seen that the expressive power of *first-order logic*, in terms of computational complexity is *weak*.

Second-order logic allows us to express all properties in the *polynomial hierarchy*.

Are there interesting logics intermediate between these two?

We have seen one—*monadic second-order logic*.

We now examine another—*LFP*—the logic of *least fixed points*.

Inductive Definitions

LFP is a logic that formalises *inductive definitions*.

> *Unlike in second-order logic, we cannot quantify over arbitrary relations, but we can build new relations inductively.*

Inductive definitions are pervasive in mathematics and computer science.

The *syntax* and *semantics* of various formal languages are typically defined inductively.

> *viz. the definitions of the syntax and semantics of first-order logic seen earlier.*

Transitive Closure

The *transitive closure* of a binary relation E is the *smallest* relation T satisfying:

- $E \subseteq T$; and
- if $(x, y) \in T$ and $(y, z) \in E$ then $(x, z) \in T$.

This constitutes an *inductive definition* of T and, as we have already seen, there is no *first-order* formula that can define T in terms of E.

Monotone Operators

In order to introduce LFP, we briefly look at the theory of *monotone operators*, in our restricted context.

We write $\mathrm{Pow}(A)$ for the powerset of A.
An operator on A is a function

$$F : \mathrm{Pow}(A) \to \mathrm{Pow}(A).$$

F is *monotone* if

$$\text{if } S \subseteq T, \text{ then } F(S) \subseteq F(T).$$

Least and Greatest Fixed Points

A *fixed point* of F is any set $S \subseteq A$ such that $F(S) = S$.

S is the *least fixed point* of F, if for all fixed points T of F, $S \subseteq T$.

S is the *greatest fixed point* of F, if for all fixed points T of F, $T \subseteq S$.

Least and Greatest Fixed Points

For any monotone operator F, define the collection of its *pre-fixed points* as:

$$Pre = \{S \subseteq A \mid F(S) \subseteq S\}.$$

Note: $A \in Pre$.

Taking

$$L = \bigcap Pre,$$

we can show that L is a fixed point of F.

Fixed Points

For any set $S \in Pre$,

$L \subseteq S$	*by definition of* L.
$F(L) \subseteq F(S)$	*by monotonicity of* F.
$F(L) \subseteq S$	*by definition of* Pre.
$F(L) \subseteq L$	*by definition of* L.
$F(F(L)) \subseteq F(L)$	*by monotonicity of* F
$F(L) \in Pre$	*by definition of* Pre.
$L \subseteq F(L)$	*by definition of* L.

Least and Greatest Fixed Points

L is a *fixed point* of F.

Every fixed point P of F is in Pre, and therefore $L \subseteq P$.

Thus, L is the least fixed point of F

Similarly, the greatest fixed point is given by:

$$G = \bigcup\{S \subseteq A \mid S \subseteq F(S)\}.$$

Iteration

Let A be a *finite* set and F be a *monotone* operator on A.

Define for $i \in \mathbb{N}$:

$$\begin{aligned} F^0 &= \emptyset \\ F^{i+1} &= F(F^i). \end{aligned}$$

For each i, $F^i \subseteq F^{i+1}$ (proved by induction).

Iteration

Proof by induction.

$$\emptyset = F^0 \subseteq F^1.$$

If $F^i \subseteq F^{i+1}$ then, by monotonicity

$$F(F^i) \subseteq F(F^{i+1})$$

and so $F^{i+1} \subseteq F^{i+2}$.

Fixed-Point by Iteration

If A has n elements, then

$$F^n = F^{n+1} = F^m \quad \text{for all} \quad m > n$$

Thus, F^n is a fixed point of F.

Let P be any fixed point of F. We can show by induction on i, that $F^i \subseteq P$.

$$F^0 = \emptyset \subseteq P$$

If $F^i \subseteq P$ then

$$F^{i+1} = F(F^i) \subseteq F(P) = P.$$

Thus F^n is the *least fixed point* of F.

Defined Operators

Suppose ϕ contains a relation symbol R (of arity k) not interpreted in the structure $\mathbb{A}$ and let $\mathbf{x}$ be a tuple of k free variables of ϕ.

For any relation $P \subseteq A^k$, ϕ defines a new relation:

$$F_P = \{\mathbf{a} \mid (\mathbb{A}, P) \models \phi[\mathbf{a}]\}.$$

The operator $F_\phi : \mathrm{Pow}(A^k) \to \mathrm{Pow}(A^k)$ defined by ϕ is given by the map

$$P \mapsto F_P.$$

Or, $F_{\phi,\mathbf{b}}$ if we fix parameters $\mathbf{b}$.

Positive Formulas

Definition

A formula ϕ is *positive* in the relation symbol R, if every occurence of R in ϕ is within the scope of an even number of negation signs.

Lemma

For any structure $\mathbb{A}$ not interpreting the symbol R, any formula ϕ which is positive in R, and any tuple $\mathbf{b}$ of elements of A, the operator $F_{\phi,\mathbf{b}} : \mathrm{Pow}(A^k) \to \mathrm{Pow}(A^k)$ is monotone.

Syntax of LFP

- Any relation symbol of arity k is a predicate expression of arity k;
- If R is a relation symbol of arity k, $\mathbf{x}$ is a tuple of variables of length k and ϕ is a formula of LFP in which the symbol R only occurs positively, then

$$\mathbf{lfp}_{R,\mathbf{x}}\phi$$

is a predicate expression of LFP of arity k.

All occurrences of R and variables in $\mathbf{x}$ in $\mathbf{lfp}_{R,\mathbf{x}}\phi$ are *bound*

Syntax of LFP

- If t_1 and t_2 are terms, then $t_1 = t_2$ is a formula of LFP.
- If P is a predicate expression of LFP of arity k and $\mathbf{t}$ is a tuple of terms of length k, then $P(\mathbf{t})$ is a formula of LFP.
- If ϕ and ψ are formulas of LFP, then so are $\phi \land \psi$, and $\neg\phi$.
- If ϕ is a formula of LFP and x is a variable then, $\exists x \phi$ is a formula of LFP.

Semantics of LFP

Let $\mathbb{A} = (A, \mathcal{I})$ be a structure with universe A, and an interpretation $\mathcal{I}$ of a fixed vocabulary σ.

Let ϕ be a formula of LFP, and $\imath$ an interpretation in A of all the free variables (*first or second* order) of ϕ.

To each individual variable x, $\imath$ associates an element of A, and to each k-ary relation symbol R in ϕ that is not in σ, $\imath$ associates a relation $\imath(R) \subseteq A^k$.

$\imath$ is extended to terms t in the usual way.

For constants c, $\imath(c) = \mathcal{I}(c)$.
$\imath(f(t_1, \ldots, t_n)) = \mathcal{I}(f)(\imath(t_1), \ldots, \imath(t_n))$

Semantics of LFP

- If R is a relation symbol in σ, then $\imath(R) = \mathcal{I}(R)$.
- If P is a predicate expression of the form $\mathbf{lfp}_{R,\mathbf{x}}\phi$, then $\imath(P)$ is the relation that is the least fixed point of the monotone operator F on A^k defined by:

$$F(X) = \{\mathbf{a} \in A^k \mid \mathbb{A} \models \phi[\imath\langle X/R, \mathbf{x}/\mathbf{a}\rangle],$$

where $\imath\langle X/R, \mathbf{x}/\mathbf{a}\rangle$ denotes the interpretation $\imath'$ which is just like $\imath$ *except* that $\imath'(R) = X$, and $\imath'(\mathbf{x}) = \mathbf{a}$.

Semantics of LFP

- If ϕ is of the form $t_1 = t_2$, then $\mathbb{A} \models \phi[\imath]$ if, $\imath(t_1) = \imath(t_2)$.
- If ϕ is of the form $R(t_1, \ldots, t_k)$, then $\mathbb{A} \models \phi[\imath]$ if,

$$(\imath(t_1), \ldots, \imath(t_k)) \in \imath(R).$$

- If ϕ is of the form $\psi_1 \land \psi_2$, then $\mathbb{A} \models \phi[\imath]$ if, $\mathbb{A} \models \psi_1[\imath]$ *and* $\mathbb{A} \models \psi_2[\imath]$.
- If ϕ is of the form $\neg\psi$ then, $\mathbb{A} \models \phi[\imath]$ if, $\mathbb{A} \not\models \psi[\imath]$.
- If ϕ is of the form $\exists x \psi$, then $\mathbb{A} \models \phi[\imath]$ if there is an $a \in A$ such that $\mathbb{A} \models \psi[\imath\langle x/a \rangle]$.

Transitive Closure

The formula (with free variables u and v)

$$\theta \quad \equiv \quad \mathbf{lfp}_{T,xy}[(x = y \vee \exists z(E(x,z) \wedge T(z,y)))](u,v)$$

defines the *reflexive and transitive closure* of the relation E.

Thus $\forall u \forall v\ \theta$ defines *connectedness*.

The expressive power of LFP properly extends that of first-order logic.

Greatest Fixed Points

If ϕ is a formula in which the relation symbol R occurs *positively*, then the *greatest fixed point* of the monotone operator F_ϕ defined by ϕ can be defined by the formula:

$$\neg[\mathbf{lfp}_{R,\mathbf{x}} \neg\phi(R/\neg R)](\mathbf{x})$$

where $\phi(R/\neg R)$ denotes the result of replacing all occurrences of R in ϕ by $\neg R$.

Exercise: Verify!.

Simultaneous Inductions

We are given two formulas $\phi_1(S, T, \mathbf{x})$ and $\phi_2(S, T, \mathbf{y})$,
S is k-ary, T is l-ary.

The pair (ϕ_1, ϕ_2) can be seen as defining a map:

$$F : \mathrm{Pow}(A^k) \times \mathrm{Pow}(A^l) \to \mathrm{Pow}(A^k) \times \mathrm{Pow}(A^l)$$

If both formulas are positive in both S and T, then there is a least fixed point.

$$(P_1, P_2)$$

defined by *simultaneous induction* on $\mathbb{A}$.

Simultaneous Inductions

Theorem

For any pair of formulas $\phi_1(S, T)$ and $\phi_2(S, T)$ of LFP, in which the symbols S and T appear only positively, there are formulas ϕ_S and ϕ_T of LFP which, on any structure $\mathbb{A}$ containing at least two elements, define the two relations that are defined on $\mathbb{A}$ by ϕ_1 and ϕ_2 by simultaneous induction.

Proof

Assume $k \leq l$.

We define P, of arity $l+2$ such that:

> $(c, d, a_1, \ldots, a_l) \in P$ *if, and only if, either* $c = d$ *and* $(a_1, \ldots, a_k) \in P_1$ *or* $c \neq d$ *and* $(a_1, \ldots, a_l) \in P_2$

For new variables x_1 and x_2 and a new $l+2$-ary symbol R, define ϕ_1' and ϕ_2' by replacing all occurrences of $S(t_1, \ldots, t_k)$ by:

$$x_1 = x_2 \wedge \exists y_{k+1}, \ldots, \exists y_l R(x_1, x_2, t_1, \ldots, t_k, y_{k+1}, \ldots, y_l),$$

and replacing all occurrences of $T(t_1, \ldots, t_l)$ by:

$$x_1 \neq x_2 \wedge R(x_1, x_2, t_1, \ldots, t_l).$$

Proof

Define ϕ as

$$(x_1 = x_2 \wedge \phi'_1) \vee (x_1 \neq x_2 \wedge \phi'_2).$$

Then,

$$(\mathbf{lfp}_{R,x_1 x_2 \mathbf{y}} \phi)(x, x, \mathbf{y})$$

defines P, so

$$\phi_S \equiv \exists x \exists y_{k+1}, \ldots, \exists y_l (\mathbf{lfp}_{R,x_1 x_2 \mathbf{y}} \phi)(x, x, \mathbf{y});$$

and

$$\phi_T \equiv \exists x_1 \exists x_2 (x_1 \neq x_2 \wedge \mathbf{lfp}_{R,x_1 x_2 \mathbf{y}} \phi)(x_1, x_2, \mathbf{y}).$$

Complexity of LFP

Any *query* definable in LFP is decidable by a *deterministic* machine in *polynomial time*.

To be precise, we can show that for each formula ϕ there is a t such that

$$\mathbb{A} \models \phi[\mathbf{a}]$$

is decidable in time $O(n^t)$ where n is the number of elements of $\mathbb{A}$.

We prove this by induction on the structure of the formula.

Complexity of LFP

- Atomic formulas by direct lookup ($O(n^a)$ time, where a is the maximum arity of any predicate symbol in σ).
- Boolean connectives are easy.

  If $\mathbb{A} \models \phi_1$ can be decided in time $O(n^{t_1})$ and $\mathbb{A} \models \phi_2$ in time $O(n^{t_2})$, then $\mathbb{A} \models \phi_1 \wedge \phi_2$ can be decided in time $O(n^{\max(t_1,t_2)})$

- If $\phi \equiv \exists x\, \psi$ then for each $a \in \mathbb{A}$ check whether

$$(\mathbb{A}, c \mapsto a) \models \psi[c/x],$$

where c is a new constant symbol. If $\mathbb{A} \models \psi$ can be decided in time $O(n^t)$, then $\mathbb{A} \models \phi$ can be decided in time $O(n^{t+1})$.

Complexity of LFP

Suppose $\phi \equiv [\mathbf{lfp}_{R,\mathbf{x}}\psi](\mathbf{t})$ (R is l-ary)

To decide $\mathbb{A} \models \phi[\mathbf{a}]$:

$R := \emptyset$
for $i := 1$ **to** n^l **do**
    $R := F_\psi(R)$
end
if $\mathbf{a} \in R$ **then** accept **else** reject

Complexity of LFP

To compute $F_\psi(R)$

For every tuple $\mathbf{a} \in A^l$*, determine whether* $(\mathbb{A}, R) \models \psi[\mathbf{a}]$.

If deciding $(\mathbb{A}, R) \models \psi$ takes time $O(n^t)$, then each assignment to R inside the loop requires time $O(n^{l+t})$. The total time taken to execute the loop is then $O(n^{2l+t})$. Finally, the last line can be done by a search through R in time $O(n^l)$. The total running time is, therefore, $O(n^{2l+t})$.

The *space* required is $O(n^l)$.

Capturing P

For any ϕ of LFP, the language $\{[\mathbb{A}]_< \mid \mathbb{A} \models \phi\}$ is in P.

Suppose ρ is a signature that contains a *binary relation symbol* $<$, possibly along with other symbols.

Let $\mathcal{O}_\rho$ denote those structures $\mathbb{A}$ in which $<$ is a *linear order* of the universe.

For any language $L \in$ P, there is a sentence ϕ of LFP that defines the class of structures

$$\{\mathbb{A} \in \mathcal{O}_\rho \mid [\mathbb{A}]_{<^{\mathbb{A}}} \in L\}$$

(Immerman; Vardi 1982)

Capturing P

Recall the proof of *Fagin's Theorem*, that ESO captures NP.

Given a machine M and an integer k, there is a *first-order* formula $\phi_{M,k}$ such that

$$\mathbb{A} \models \exists < \exists T_{\sigma_1} \cdots T_{\sigma_s} \exists S_{q_1} \cdots S_{q_m} \exists H \, \phi_{M,k}$$

if, and only if, M accepts $[\mathbb{A}]_<$ in time n^k, for some order $<$.

If we *fix* the order $<$ as part of the structure $\mathbb{A}$, we do not need the outermost quantifier.

Moreover, for a *deterministic* machine M, the relations $T_{\sigma_1} \ldots T_{\sigma_s}, S_{q_1} \ldots S_{q_m}, H$ can be defined *inductively*.

Capturing P

$$
\begin{aligned}
&\mathsf{Tape}_a(\mathbf{x},\mathbf{y}) \Leftrightarrow\\
&(\mathbf{x} = \mathbf{1} \wedge \mathrm{Init}_a(\mathbf{y}))\vee\\
&\ \exists \mathbf{t} \exists \mathbf{h} \bigvee_q \quad (\mathbf{x} = \mathbf{t}+1 \wedge \mathsf{State}_q(\mathbf{t},\mathbf{h})\wedge\\
&\qquad\qquad [(\mathbf{h} = \mathbf{y} \wedge \bigvee_{\{b,d,q' \mid \Delta(q,b,q',a,d)\}} \mathsf{Tape}_b(\mathbf{t},\mathbf{y})\vee\\
&\qquad\qquad \mathbf{h} \neq \mathbf{y} \wedge \mathsf{Tape}_a(\mathbf{t},\mathbf{y})]);
\end{aligned}
$$

where $\mathrm{Init}_a(\mathbf{y})$ is the formula that defines the positions in which the symbol a appears in the input.

Capturing P

$$
\begin{array}{lll}
\multicolumn{3}{l}{\mathrm{State}_q(\mathbf{x},\mathbf{y}) \Leftrightarrow} \\
\multicolumn{3}{l}{(\mathbf{x} = \mathbf{1} \land \mathbf{y} = \mathbf{1} \land q = q_0) \lor} \\
\exists \mathbf{t} \exists \mathbf{h} & \bigvee_{\{a,b,q' \mid \Delta(q',a,q,b,R)\}} & \big(\mathbf{x} = \mathbf{t}+1 \land \mathrm{State}_{q'}(\mathbf{t},\mathbf{h}) \land \\
& & \mathrm{Tape}_a(\mathbf{t},\mathbf{h}) \land \mathbf{y} = \mathbf{h}+1)\big) \\
& \bigvee_{\{a,b,q' \mid \Delta(q',a,q,b,L)\}} & \big(\mathbf{x} = \mathbf{t}+1 \land \mathrm{State}'_q(\mathbf{t},\mathbf{h}) \land \\
& & \mathrm{Tape}_a(\mathbf{t},\mathbf{h}) \land \mathbf{h} = \mathbf{y}+1)\big).
\end{array}
$$

Unordered Structures

In the absence of an *order relation*, there are properties in P that are not definable in LFP.

There is no sentence of LFP which defines the structures with an *even* number of elements.

Evenness

Let $\mathcal{E}$ be the collection of all structures in the empty signature.

In order to prove that *evenness* is not defined by any LFP sentence, we show the following.

Lemma
For every LFP formula ϕ there is a first order formula ψ, such that for all structures $\mathbb{A}$ in $\mathcal{E}$, $\mathbb{A} \models (\phi \leftrightarrow \psi)$.

Unordered Structures

Let $\psi(\mathbf{x}, \mathbf{y})$ be a first order formula.

$\mathbf{lfp}_{R,\mathbf{x}}\psi$ defines the relation

$$F^{\infty}_{\psi,\mathbf{b}} = \bigcup_{i \in \mathbb{N}} F^{i}_{\psi,\mathbf{b}}$$

for a fixed interpretation of the variables $\mathbf{y}$ by the tuple of parameters $\mathbf{b}$.

For each i, there is a first order formula ψ^i such that on any structure $\mathbb{A}$,

$$F^{i}_{\psi,\mathbf{b}} = \{\mathbf{a} \mid \mathbb{A} \models \psi^i[\mathbf{a}, \mathbf{b}]\}.$$

Defining the Stages

These formulas are obtained by *induction*.

> ψ^1 *is obtained from* ψ *by replacing all occurrences of subformulas of the form* $R(\mathbf{t})$ *by* $t \neq t$.
>
> ψ^{i+1} *is obtained by replacing in* ψ, *all subformulas of the form* $R(\mathbf{t})$ *by* $\psi^i(\mathbf{t}, \mathbf{y})$

Let $\mathbf{b}$ be an l-tuple, and $\mathbf{a}$ and $\mathbf{c}$ two k-tuples in a structure $\mathbb{A}$ such that *there is an automorphism* $\imath$ *of* $\mathbb{A}$ (i.e. an *isomorphism* from $\mathbb{A}$ to itself) such that

- $\imath(\mathbf{b}) = \mathbf{b}$
- $\imath(\mathbf{a}) = \mathbf{c}$

Then,

$$\mathbf{a} \in F^{i}_{\psi,\mathbf{b}} \quad \text{if, and only if,} \quad \mathbf{c} \in F^{i}_{\psi,\mathbf{b}}.$$

Bounding the Induction

This defines an *equivalence relation* $\mathbf{a} \sim_{\mathbf{b}} \mathbf{c}$.

If there are p distinct equivalence classes, then

$$F^{\infty}_{\psi,\mathbf{b}} = F^{p}_{\psi,\mathbf{b}}$$

In $\mathcal{E}$ there is a uniform bound p, that does not depend on the size of the structure.